BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan meningkatnya jumlah pengguna internet di Indonesia telah membawa kemudahan sekaligus tantangan baru dalam perlindungan data pribadi. Sebagaimana dibahas dalam jurnal *Urgensi Perlindungan Data Pribadi dalam Perspektif Hak Asasi Manusia*, maraknya kasus kebocoran data di berbagai platform digital seperti Tokopedia, Bhineka.com, dan Bukalapak menunjukkan bahwa informasi perseorangan menjadi akar dari banyak permasalahan hukum dan sosial. Penelitian tersebut menegaskan bahwa perlindungan data pribadi merupakan bagian dari hak asasi manusia yang dijamin dalam Pasal 28G ayat (1) UUD 1945, namun regulasi yang ada masih bersifat parsial dan belum mampu memberikan perlindungan komprehensif. Kondisi ini diperparah dengan rendahnya efektivitas implementasi regulasi yang ada, sehingga masyarakat tetap rentan terhadap penyalahgunaan data pribadi. Hal ini menegaskan pentingnya pembentukan mekanisme hukum yang lebih jelas serta sistem pengawasan yang efektif untuk melindungi masyarakat dari ancaman kebocoran data[1].

Sejalan dengan permasalahan regulasi tersebut, penelitian lain yang berjudul *Kejahatan Siber Terhadap Individu: Jenis, Analisis, dan Perkembangannya* menyoroti bahwa tidak hanya organisasi maupun kelompok, namun individu juga merupakan target utama dalam berbagai bentuk kejahatan siber. Jenis kejahatan yang paling sering terjadi meliputi rekayasa sosial, pencurian identitas, peretasan, pelecehan daring, hingga penolakan layanan. Faktor manusia menjadi titik lemah yang paling banyak dieksploitasi oleh pelaku, sehingga kebocoran data pribadi tidak hanya menimbulkan kerugian finansial, tetapi juga berdampak pada privasi, reputasi, dan kesejahteraan psikologis korban[2].

Kemudian dalam penelitian *Cybercrime in the new criminal code in Indonesia* menunjukkan bahwa kebocoran data pribadi dan kejahatan siber lainnya

semakin meningkat pesat di era *Society 5.0*, di mana teknologi seperti *Artificial Intelligence (AI)*, *Internet of Things (IoT)*, dan *big data* digunakan secara luas dalam kehidupan sehari-hari. KUHP baru yang disahkan pada tahun 2023 bersama dengan amandemen UU ITE tahun 2024 menegaskan perlunya kerangka hukum pidana yang lebih adaptif terhadap kejahatan digital, termasuk akses ilegal, pencurian data, penyadapan, hingga penyalahgunaan teknologi AI seperti *deepfake*. Kemudian pada penelitian tersebut juga menyoroti bahwa meskipun regulasi hukum telah diperbarui, tantangan besar tetap ada, seperti kecepatan inovasi teknologi yang melampaui pembaruan hukum, keterbatasan kapasitas aparat penegak hukum, serta rendahnya kesadaran publik mengenai keamanan digital. Kondisi ini memperlihatkan bahwa kebocoran data pribadi bukan hanya masalah teknis, tetapi juga menyangkut aspek hukum, sosial, dan ekonomi yang saling berkaitan[3].

Sejalan dengan berbagai kajian tersebut, penelitian berjudul *Private Investigation and Open Source Intelligence (OSINT)* menekankan bahwa kebocoran data pribadi tidak hanya dapat dipahami dari sisi regulasi maupun dampak sosial, tetapi juga perlu dianalisis melalui pendekatan teknis investigasi. OSINT sebagai metode pengumpulan dan analisis informasi dari sumber terbuka terbukti mampu mengidentifikasi pola kebocoran data, aktivitas ilegal, hingga penyalahgunaan identitas secara sistematis[4]. Kerentanan terbesar bagi individu seringkali muncul dari *Passive Digital Footprint* data pribadi sensitif (PII) yang terekspos secara tidak disengaja melalui dokumen atau entri basis data lama yang terindeks di mesin pencari. Oleh karena itu, penelitian ini berfokus pada analisis kebocoran data sensitif perseorangan menggunakan OSINT Hibrida (kombinasi OSINT Dorking dan *Social Media Intelligence*) untuk mendemonstrasikan efektivitasnya dalam memetakan dan menganalisis risiko eksploitasi data pribadi yang mengarah pada ancaman *doxing* dan *penipuan* pada tingkat individu.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang diatas, maka rumusan masalahyang akan diselesaikan dalam penelitian ini yaitu :

1. Jenis PII sensitif apa saja yang berhasil diidentifikasi dan divalidasi

menggunakan teknik OSINT Hibrida (Dorking dan SOCMINT)?

2. Bagaimana korelasi PII sensitif tersebut secara langsung mendemonstrasikan potensi risiko eksploitasi *Doxing* dan ancaman pada tingkat individu melalui uji simulasi kerentanan?

1.3 Batasan Masalah

Agar penelitian ini berjalan dengan terarah dan terstruktur, maka berdasarkan pemaparan rumusan masalah sebelumnya, peneliti membuat batasan masalah. Batasan masalah yang ditetapkan dalam penelitian ini adalah sebagai berikut :

1. Peneliti membatasi pengumpulan data pada implementasi OSINT Hibrida melalui teknik Dorking (untuk *Passive Digital Footprint*) dan *Social Media Intelligence* (SOCMINT). Penggunaan GEOINT hanya terbatas pada validasi lokasi data PII yang bocor.
2. Pelaksanaan penelitian ini untuk menganalisis profil keamanan profil media social Instagram milik Ghina dan Niswati.
3. Peneliti melakukan *Digital Information Gathering* untuk mendapatkan data yang dibutuhkan.
4. Validasi data hanya menggunakan *tools Open Source* spesifik dan Web Open Source untuk *cross-validation* dan pengujian PII (bukan *penetration testing* sistem).

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengidentifikasi dan mengkorelasikan temuan PII sensitif yang terekspos menggunakan teknik OSINT Hibrida serta menganalisis dan mendemonstrasikan potensi risiko eksploitasi *doxing* dan *Social Engineering* (penipuan) pada tingkat individu berdasarkan temuan PII yang terkorelasi melalui uji simulasi kerentanan

1.5 Manfaat Penelitian

Meningkatkan kesadaran (*awareness*) publik mengenai risiko serius eksposur data pribadi sensitif (termasuk potensi *doxing* dan penipuan) yang berasal dari dokumen digital yang tidak terkelola dengan baik.

1.6 Sistematika Penulisan

Sistematika penulisan berisikan garis besar atau gambaran secara umum penelitian ini sehingga mempermudah pemahaman alur isi. Adapun garis besar isi skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN, tahapan ini merupakan bab awal yang menjelaskan tentang latar belakang , masalah penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penyajian.

BAB II LANDASAN TEORI, bab ini menjelaskan tinjauan kepustakaan dari penelitian-penelitian terkait yang membahas beberapa teori antara lain; apa itu OSINT, teknik OSINT (google *dorking*, profiling media sosial, *footprinting*), PII, dan *sock puppets*.

BAB III METODE PENELITIAN, bab ini berisikan Gambaran umum tentang alur dari penelitian, prosedur, dan mekanisme metode analisis yang diterapkan pada penelitian.

BAB IV HASIL DAN PEMBAHASAN, bab ini menyajikan seluruh temuan data PII sensitif hasil *Data Collection* dan *Data Processing & Validation*. Bab ini juga memuat proses *Data Correlation & Profiling* yang menghasilkan profil utuh. Pembahasan diarahkan untuk memaparkan hasil *Risk Analysis & Production* melalui uji simulasi kerentanan dan membandingkan temuan dengan literatur terdahulu untuk menjawab tujuan penelitian.

BAB V PENUTUP, berisi kesimpulan yang merupakan jawaban final atas rumusan masalah penelitian (terkait efektivitas OSINT dan tingkat risiko PII yang bocor), serta memuat saran yang dirangkum berdasarkan hasil analisis risiko.